第 37 卷第 1 期 计算机应用研究 Vol. 37 No. 1
录用定稿 Application Research of Computers Accepted Paper

基于双线性映射的三因子远程身份认证协议研究 *

魏春英，郭中华

(宁夏大学 物理与电子电气工程学院，银川 750021)

摘　要：为了提高多服务器环境身份认证的安全性，降低计算复杂度，提出一种基于双线性映射的三因子认证协议，这些因子包括生物信息、智能卡和双线性映射密码。所提协议包括系统设置、服务器注册、用户注册、登录、认证和密钥协商，以及密码更新六个阶段，其中，生物因子和智能卡作为核心因子涉及注册、登录和认证和更改阶段。Oracle 形式化证明验证了所提协议的安全性，攻击者无法得到标志、密码、生物特征信息等，可以实现密钥协商和双向身份认证。与其他相关协议相比，所提协议在安全特征、智能卡存储成本、通信成本等方面具有一定优势。

关键词：多服务器；身份认证；双线性映射；生物信息；智能卡；形式化证明

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.06.0476

Research of three factor remote authentication protocol based on bilinear mapping

Wei Chunying, Guo Zhonghua

(*College of Physics & Electronic Electrical Engineering Ningxia University*, *Yinchuan* 750021, *China*)

Abstract: To improve the security of authentication in multiple-server environment and reduce the computational complexity, a three factor authentication protocol based on bilinear mapping is proposed, which includes three factors of bioinformatics, smart card and bilinear mapping cipher. The proposed protocol includes 6 stages: system setup, server registration, user registration, login, authentication and key agreement, and password update. Among them, biological factors and smart cards as the core factors involve registration, landing, authentication and modification. Formal verification of Oracle verifies the security of the protocol. Attackers can not get identification, password, biometric information, etc. , and this achieves key agreement and mutual authentication. Compared with other related protocols, the proposed protocol has some advantages in security features, smart card storage cost, communication cost and so on.

Key words: multiple-server; authentication; bilinear mapping; bioinformatics; smart card; formal verification

0　引言

现代网络通信技术的迅猛发展使得在线服务[1]的功能大量增加，服务质量大幅提高。诸如电子邮件、电子医疗、网上银行和商务已经成为人们日常生活的重要组成部分。然而，这些在线服务大多在不可信信道上进行，造成不法分子的有机可乘。因此，因此在线服务的隐私性、完整性、保密性等安全性问题至关重要，其中，身份认证[2]是在线服务的重要前提，是网络安全性的研究热点和难点。

按照服务器的分布性，身份认证协议可分为单服务器环境和多服务器环境。单服务器环境中，用户必须注册到每个应用服务器，其最大缺点是用户必须记住多个服务器对应的密码和标志，用户体验较差，这种情况适用于一些特别安全考虑的情形，如某些健康安全系统[3]。多服务器环境则不需要这样繁琐，单次注册即可访问多个服务器。

多服务器环境的身份认证研究得较广，如文献[4]提出了一种基于多服务器环境的鲁棒双因子认证协议，即智能卡和曲线密码，该协议能够抵御多种潜在的网络攻击。文献[5]研究了文献[4]的协议，证明其存在安全漏洞。易受假冒攻击、密码猜测攻击和特权内部者攻击，并提出了克服上述缺陷改进的双因子协议。相关研究表明[6]，双因子认证协议可靠性不足，因为用户通常会选择一个低熵密码，易受字典攻击。文献[7]针对当前跨信任域密钥协商协议无法满足网络需求的问题，提出一种跨身份的自治域密钥协商协议，使用不同的公开参数和 PKG 主密钥，该协议所使用的因子较少。文献[8]指出研究了文献[9]的身份认证协议，指出其易受智能卡丢失攻击、服务器模仿攻击等缺点，难以保护用户的隐私性。并基于生物特征和扩展混沌映射，提出了一个改进的身份认证协议。

当前很多研究者为了降低复杂度，使用了双线性配对或点乘用于身份认证，本文也运用了双线性配对，提出了一种基于

收稿日期：2018-06-21；**修回日期：**2018-09-14　　**基金项目：**国家自然基金资助项目（61565014）

作者简介：魏春英（1975-），女，宁夏银川人，副教授，硕士，主要研究方向为信息安全、物联网等；郭中华（1973-），男，宁夏银川人，教授，博士，主要研究方向为网络安全、密码学、电路设计应用等.

双线性映射[10]的三因子远程身份认证协议，这些因子包括生物因子、智能卡和密码，分析结果表明所提协议具有较高的安全性和计算效率。

1　提出的远程身份认证协议

1.1　系统设置阶段

注册中心 RC 选择一个随机数 $S_{RS} \in Z_q^*$，并保留该随机数作为密钥。其计算 $Pub_{RS} = S_{RS} \cdot P$，式中 P 为组 G_1 的生成器。RC 将{ê, G_1, G_2, q, P, Pub_{RS}, $H(.)$, $h(.)$}声明为公共参数。

1.2　服务器注册阶段

该阶段中，一个新的应用服务器 SS_j 加入多服务器环境以向远程用户 U_i 提供服务。服务器 SS_j 选择一个身份标志 SID_j（$1<j<m$），其中，m 表示多服务器环境中包含的 SS_j 总数量。服务器 SS_j 将 SID_j 发送到注册中心 RC。在接收到来自 SS_j 的 SID_j 后，RC 计算 $S_j = h(SID_j \| S_{RS}) \cdot P \in G_1$，$Pub_j = S_j \cdot P \in G_1$，然后，通过一个可靠信道将 S_j 发送到应用服务器 SS_j，并公开 Pub_j 作为公共参数。

1.3　用户注册阶段

当远程用户 U_i 希望接入 SS_j 的服务时，U_i 需要通过以下步骤注册到 RC。

a)用户 U_i 选择 ID_i 和 PW_i，并在传感器输入其生物特征 B_i，U_i 计算 $UID_i = H(ID_i) \in G_1$ 和 $HPW_i = h(PW_i \| ID_i) \cdot P \in G_1$，通过一个可信信道将{$UID_i$, HPW_i, B_i}发送到 RC。

b)在收到来自 U_i 的注册消息后，RC 计算 $b_i = H_1(B_i)$，$Reg_i = h(UID_i \| HPW_i) \in Z_q^*$，$DID_i = S_{RS} \cdot UID_i \in G_1$，$Z_i = h(HPW_i) \cdot P \in G_1$ 以及 $S_i = DID_i + Z_i \in G_1$。$RC$ 为每个用户每次生成一个唯一表示（TID_i），并计算 $PID_i = h(TID_i \| S_{RS})$。其后，RC 在数据库中存储{$PID_i$, UID_i}和状态位(0, 1)，其中状态位表示用户的状态。最后，RC 生成一张包含信息 {TID_i, b_i, Reg_i, S_i, Pub_{RS}, $H(.)$, $h(.)$, $H1$}的智能卡，并通过一个可靠信道将其发送至 U_i。

1.4　登录阶段

当用户 U_i 希望登录到服务器 SS_j 时，需要执行以下步骤:

a)U_i 将智能卡插入终端，输入 ID_i^*、PW_i^* 和 B_i^*。智能卡读卡器计算 $UID_i^* = H(ID_i^*)$，$HPW_i^* = h(PW_i^* \| ID_i^*) \cdot P$，和 $b_i^* = H_1(B_i)$，并检查 $b_i^* = b_i$ 是否成立。若成立，则意味着用户 U_i 输入了正确的生物统计信息；若不成立，则中止连接。此后，智能卡计算 $Reg_i^* = h(UID_i^* \| HPW_i^*)$，并将其与存储的 Reg_i 进行比较。若两者匹配，则确认 U_i 输入了正确的{ID_i, PW_i}，并进入下一步骤。

b)智能卡生成一个随机数 r_i，并计算 $Z_i = h(HPW_i) \cdot P \in G_1$，$DID_i = S_i - Z_i \in G_1$，$R_i = r_i \cdot P \in G_1$，$M_i = r_i \cdot Pub_{RS} \in G_1$，和 $d_i = h(UID_i \| SID_i \| M_i \| DID_i) \in Z_q^*$。最后，智能卡读卡器将登陆消息 M_1={R_i, TID_i, SID_j, d_i}通过一个不可靠信道发送给 RC。

1.5　验证和密钥协商阶段

该阶段中执行以下步骤:

a) 在收到来自用户的登陆消息 M_1 后，RC 计算 $PID_i^* = h(TID_i \| S_{RS})$，并检查数据库中是否存在 PID_i^*。若不存在，则 RC 退出会话；若存在，RC 从数据库中得到 UID_i 并进入下一步骤。

b)RC 计算 $M_i^* = R_i \cdot S_{RS} = M_i$，$DID_i^* = UID_i \cdot S_{RS}$ 和 $d_i^* = h(UID_i \| SID_j \| M_i^* \| DID_i^*)$，并检查 $d_i^* = d_i$ 和 $\hat{e} < UID_i, Pub_{RS} > = \hat{e} < DID_i, P >$ 是否成立。若两个条件均成立，则 RC 执行下一个步骤；否则，会话将被终止。

c)RC 生成一个随机 nonce n_i，并计算 $S_j = h(SID_j \| S_{RS}) \cdot P \in G_1$，$L_i = n_i \cdot P$，$w_i = n_i \cdot Pub_j$，$k_j = UID + w_i$，以及 $T_i = h(UID_i \| SID_j \| S_j \| w_i)$。随后，$RC$ 通过一个公共信道将 M_2 ={L_i, K_i, SID_j, T_i}发送给 SS_j。

d)在接收到来自 RC 的消息 M_2 后，SS_j 计算 $w_i^* = L_i \cdot S_j = w_i$，$UID_i = K_i - w_i^* \in G_1$，以及 $T_i^* = h(UID_i \| SID_j \| S_j \| w_i^*) \in Z_q^*$，并检查 $T_i^* = T_i$ 是否成立。若成立，则用户 U_i 和注册中心 RC 对于服务器 SS_j 是可信的；若不成立，则终止会话。此后，SS_j 生成 c_i，并计算 $y_i = c_i \cdot P \in G_1$，$D_i = y_i + UID_i \in G_1$，$G_i = h(y_i \| UID_i) \in Z_q^*$ 和 $E_i = h(UID_i \| SID_j \| y_i \| G_i) \in Z_q^*$，通过一个不可靠信道将 M_3 ={SID_j, K_i, D_i, E_i}发送给用户 U_i。

e)在接收到来自 SS_j 的消息 M_3 后，U_i 计算 $y_i^* = D_i - UID_i$，$w_i^* = K_i - UID_i$，$G_i^* = h(y_i^* \| UID_i)$，以及 $E_i^* = h(UID_i \| SID_j \| y_i^* \| G_i^*)$，并检查 $E_i^* = E_i$ 是否成立。若成立，则 RC 和 SS_j 通过 U_i 的身份验证。此外，用户 U_i 计算 $SK = h(UID_i \| SID_j \| M_i \| y_i^* \| w_i^*)$，$O_i = M_i + y_i^*$ 以及 $V_i = h(O_i \| SK)$，并通过一个不可靠信道将消息 M_4={V_i, O_i}发送至 SS_j。

f)在接收到来自 U_i 的消息 M_4 后，服务器计算 $M_i^* = O_i - y_i$，$SK^* = h(UID_i \| SID_j \| M_i^* \| y_i \| w_i^*)$，以及 $V_i^* = h(O_i \| SK)$，并检查 $V_i^* = V_i$ 是否成立。若成立，则会话密钥有效，SS_j 和 U_i 就可以使用该共享密钥 SK 相互通信；若不成立，则会话被终止。

1.6　密码更改阶段

该阶段中，用户能够通过执行以下步骤，在不需要注册中心任何帮助的情况下，将旧密码 PW_i 替换为新密码 PW_i^{new}。

a)用户 U_i 将智能卡插入终端，并在特定设备上输入{ID_i, PW_i}和生物统计信息 B_i。

b) 智能卡计算 $UID_i = H(ID_i) \in G_1$，$HPW_i = h(PW_i^* \| ID_i^*) \cdot P \in G_1$，以及 $b_i^* = H_1(B_i)$，并检查 $b_i^* = b_i$ 是否成立。若成立，则意味着 U_i 输入了正确的生物统计信息；若不成立，则中止会话。

c)智能卡计算 $Reg_i^* = h(UID_i \| HPW_i)$，并检查 $Reg_i^* = Reg_i$ 是否成立。若不成立，则智能卡拒绝密码更改请求；若成立，智能卡要求用户 U_i 输入一个新的密码 PW_i^{new}。

d) 智能卡计算 $DID_i = S_i - Z_i = S_{RS} \cdot UID_i$，$HPW^{new} = H(PW_i^{new} \| ID_i) \cdot P$，$Reg_i^{new} = h(UID_i \| HPW^{new})$，$Z_i^{new} = h(HPW^{new}) \cdot P$，以及 $S_i^{new} = DID_i + Z_i^{new}$。最后，智能卡将其存储器中旧的{$Reg_i$, S_i}替换为{Reg_i^{new}, S_i^{new}}，至此密码更改

阶段成功完成。

2　Oracle 形式化安全证明

本章将使用随机 Oracle 模型[11]（ROM）的形式化安全分析，对于本文协议，证明攻击者 A 无法得到标志 ID_i、密码 PW_i、生物特征 B_i 和会话密钥 SK。本文首先在定义 1~4 中分别解释可忽略函数、抗冲突特性和 Reveal oracle，其后将证明这些定理。

定义 1　可忽略函数　对于所有正整数 d，若存在一个整数 k_0，使得对于每个 $k \geq k_0$，$h(k) < k^{-d}$，那么 $h(k) < k^{-d}$ 被称为可忽略函数。

定义 2　抗冲突特性　抗冲突定义是 $Adv_{\mathcal{A}}^{H}(t) = prb(re, re') \Leftarrow =_R \mathcal{A}$ 以及 $h(re) = h(re')$，式中，$prb(re, re')$ 表示事件 (re, re') 的成功概率，$\Leftarrow =_R \mathcal{A}$ 表示 A 所选择的事件 (re, re')，$Adv_{\mathcal{A}}^{H}(t)$ 表示在时间周期 t 中事件 (re, re') 的优势函数。

定义 3　*Reveal* 1　该 Reveal Oracle 无条件从散列输出 y 中提供输入 re，即 $y = h(re)$。

定义 4　*Reveal* 2　已知 $G \in E_p(a,b)$ 和公共参数 $Q = x \cdot G \in E_p(a,b)$，则该 oracle 输出私有密钥 x。

定理 1　假定不可逆散列函数作为一个随机 oracle，A 知晓通信消息$\{SID_j, Y_i, K_i, V_i\}$。那么 A 依然无法检索 ID_i 和会话密钥 SK。

证明　首先，假定 A 能够借助实验性算法“多服务器三因子远程认证方案的密码分析和改进[12]（CITRASM）”检索 ID_i 和 SK。则 CITRASM 的成功概率表示如下：

$$Success1 = \left| Pr[Exp1_{\mathcal{A},CITRASM}^{HASH} = 1] - 1 \right| \quad (1)$$

其中：$Pr(.)$表示算法 1 的成功概率。此后，本文将 $Exp1_{\mathcal{A},CITRASM}^{HASH}$ 的优势定义为

$$Adv1(t_1, q_{r1}) = Max_{\mathcal{A}}\{Success1\} \quad (2)$$

其中：最大值取决于 Reveal Oracle 在时间区间 t_1 中所执行的查询 q_{r1} 的数量。

若 $Adv1(t_1, q_{r1}) > \varepsilon$，其中 $\varepsilon > 0$，则攻击者能够检索 U_i 的 ID_i 和 SK。该条件仅在攻击者能够对不可逆散列函数进行求逆的情况下才成立[13]。由于从散列函数中检索到的输入不具备计算可行性，即，$Adv1(t_1, q_{r1}) < \varepsilon$。因此，提出的方案能够阻止 A 得到 U_i 的 ID_i 和会话密钥 SK。

算法 1　$Exp1_{\mathcal{A},CITRASM}^{HASH}$

1. 输入：$< SID_j, Y_i, K_i, G, V_i >$
2. 结果：1 或 0
3. 在 K_i 上应用 Reveal Oracle，以得到信息 P_i，W_i，ID_i，SID_j，以及 RS_j，即
   $$(P_i^* \| W_i^* \| ID_i^* \| SID_j^* \| RS_j^*) \leftarrow Reveal1(K_i)$$
4. 计算 $Y_i^* = P_i^* + h(ID_i^* \| W_i^*) \cdot G$
5. **if** $(Y_i^* = Y_i)$ 且 $(SID_j^* = SID_j)$，**then**
6. 　　ID_i^* 为用户 U_i 的正确身份标志
7. 　　在 V_i 上应用 Reveal Oracle 以得到 ID_i 和 SK，　即：
   $$(ID_i^{**} \| SK^*) \leftarrow Reveal1(V_i)$$
8. 　　**if** $(ID_i^* = ID_i^{**})$ **then**
9. 　　　　SK^*为正确的会话密钥
10. 　　　　Return 1 True
11. 　　**else**
12. 　　　　Return 0 False
13. 　　end if
14. else
15. 　　Return 0 False
16. end if

定理 2　假定散列函数作为一个随机 oracle，A 得到了智能卡参数 C_i、E_i、G 和通信消息 D_i、SID_i、DID_i、T_i。A 依然无法计算出用户的密码 PW_i，生物特征密钥 SP_i 和私有密钥 x。

证明　该证明与定理 1 相似。假定 A 能够计算用户的密码 PW_i、生物特征密钥 SP_i 和私有密钥 x。A 从公开信道上得到通信消息$\{D_i, SID_i, DID_i, T_i\}$，并从智能卡中提取数值$\{C_i, E_i, G\}$。那么，$A$ 执行算法以计算 PW_i，SP_i 和 x。$Exp2_{\mathcal{A},CITRASM}^{HASH}$ 的成功概率定义如下：

$$Success2 = \left| Pr[Exp2_{\mathcal{A},CITRASM}^{HASH} = 1] - 1 \right| \quad (3)$$

那么，算法 $Exp2_{\mathcal{A},CITRASM}^{HASH}$ 的优势函数定义如下：

$$Adv2(t_2, q_{r2}) = Max_{\mathcal{A}}\{Success2\} \quad (4)$$

其中：最大值取决于 Reveal Oracle 在时间区间 t_2 中所执行的查询 q_{r2} 的数量。

若 $Adv2(t_2, q_{r2}) > \varepsilon$，其中 $\varepsilon > 0$，则攻击者能够计算 PW_i、SP_i 和 x。该条件仅在攻击者能够对不可逆散列函数进行求逆的情况下才成立。由于从散列函数中推导出到的输入在多项式时间内不具备计算的可行性，这说明了 $Adv2(t_2, q_{r2}) < \varepsilon$。因此，提出的方案能够阻止 A 得到 PW_i、SP_i 和 x。

算法 2：$Exp2_{\mathcal{A},CITRASM}^{HASH}$

1. 输入：$< SID_j, G, D_i, DID_i, T_i, C_i, E_i >$
2. 结果：1 或 0
3. 在输入 D_i 上应用 Reveal Oracle，以得到信息 SID_j，ID_i，P_i 和 A_i，即 $(SID_j^* \| ID_i^* \| P_i^* \| A_i^*) \leftarrow Reveal1(D_i)$
4. 计算 $DID_i^* = ID_i^* \oplus h(P_i^* \| A_i^*)$
5. **if** $(DID_i^* = DID_i)$ 且 $(SID_j^* = SID_j)$ **then**
6. 　　在 $A_i^* = (x \cdot G)$ 上应用 Reveal Oracle，以得到信息 x，即 $x^* \leftarrow Reveal2(A_i^*)$
7. 　　计算 $P_i^{**} = T_i \cdot x^*$
8. 　　**if** $(P_i^{**} = P_i^*)$ **then**
9. 　　　　x^* 是 RC 正确的私有密钥
10. 　　　　计算 $C_i - x^* \cdot G$，其等于 $h(ID_i \| RPW_i) \cdot G$
11. 　　　　在 $(h(ID_i \| RPW_i) \cdot G)$ 上应用 Reveal Oracle，以得到信息 $(h(ID_i \| RPW_i))$，即：
    $$(h(ID_i \| RPW_i)^*) \leftarrow Reveal2(h(ID_i \| RPW_i) \cdot G)$$
    在 $(h(ID_i \| RPW_i)^*)$ 上应用 Reveal Oracle，以得到信息 ID_i

和 RPW_i，即：

$(ID_i^{**} \| RPW_i^*) \leftarrow Reveal1(h(ID_i \| RPW_i) \cdot G$

if $(ID_i^{**} = ID_i^*)$ then

在 RPW_i^* 上应用 Reveal oracle，以得到信息 PW_i 和 SP_i，即 $h(PW_i^* \| SP_i^*)Reveal1(RPW_i^*)$

计算 $E_i^* = h(h(ID_i^*) \| h(h(PW_i^* \| SP_i^*)) \bmod n_0)$

if $(E_i^* = E_i)$ then

PW_i^* 为 U_i 的正确密码，SP_i^* 为 U_i 的正确生物特征密钥

Return 1 //True

else

Return 0 //False

end if

else

Return 0 //False

end if

else

Return 0 //False

end if

else

Return 0 //False

end if

3 性能分析

本章将给出所提协议与几种相关协议在安全特征、智能卡存储成本、通信成本、计算开销和估计时间方面的性能比较。

3.1 智能卡存储成本和通信成本比较

表 1 给出了所提协议与其他协议在智能卡存储和通信成本（bit）上的比较。为评价智能卡存储和通信成本，本文考虑了 ID_i、PW_i、随机 nonce、散列函数均为 160 位，假定密钥加密或解密运算为 512 位。由表 1 可知，协议[4,5]的智能卡存储成本和通信成本低于所提协议，但两种双因子协议[4, 5]不能抵御一些安全攻击，例如用户不可跟踪性、特权内部者等。且不能提供一些安全特性，例如用户匿名性、前向加密性、高效的登录阶段和密码更改阶段。因此，付出一些额外成本得到更好的安全特性和功能是有必要的。

表 1　智能卡存储成本和通信成本比较(/bits)

Table 1　Comparison of smart card storage cost and communication cost /bit

协议	智能卡存储成本	通信成本
双因子认证[4]	640	2200
双因子改进[5]	724	2230
跨身份认证[7]	2640	2680
三因子认证[9]	1490	3460
三因子改进[8]	1520	2710
本文协议	1380	2240

3.2 安全性比较

抵御密码猜测攻击、用户匿名性、抵御服务器假冒攻击、抵御特权内部者攻击、抵御智能卡丢失攻击、提供前向保密性、抵御用户不可追踪性攻击和抵御会话密钥恢复攻击分别用 A1~A8 表示。由表 2 可知，文献[4]易受到密码猜测攻击、特权内部攻击和服务器假冒攻击，其易受的攻击类型最多。文献[5]是文献[4]的改进型，可以抵御 A1、A3 和 A4 攻击，但难以抵御用户不可追踪性攻击和密钥恢复攻击。文献[8]是文献[9]的改进型，文献[8]在抵御智能卡丢失攻击时更加可靠。对于这八种攻击，文献[8,9]都表现出不错的安全性。文献[7]次之，其没有使用智能卡因子，加强了密码因子。本文协议具有提供了更好的安全保障，可以抵御更多的攻击，具有良好的安全性。本文没有列举其他更多类型的攻击。

表 2　安全特性比较

Table 2　Comparison of safety characteristics

协议	文献[4]	文献[5]	文献[7]	文献[8]	文献[9]	本文协议
A1	No	Yes	Yes	No	No	Yes
A2	Yes	Yes	Yes	Yes	Yes	Yes
A3	No	Yes	Yes	Yes	Yes	Yes
A4	No	Yes	Yes	Yes	Yes	Yes
A5	Yes	Yes	No	Yes	No	Yes
A6	Yes	Yes	Yes	Yes	Yes	Yes
A7	No	No	No	Yes	Yes	Yes
A8	No	No	No	Yes	Yes	Yes

3.3 计算成本和估计时间比较

为了更准确比较计算成本，本文首先定义一些符号，具体如表 3 所示，表 3 还给出了一些单次计算时间，这些时间数据来自文献[14]。

表 3　符号定义

Table 3　Symbolic definition

符号	符号定义	单次计算时间/s
T_h	散列函数	0.0005
T_{me}	模指数运算	0.522
T_s	对称密钥加密(解密运算)	0.0087
T_{bh}	生物特征-散列函数	0.02102
T_{fe}	模糊提取器运算	0.0503
T_{pm}	双线性映射运算	0.0621
T_{bp}	点乘运算	0.0503

所提协议在注册阶段和登录验证阶段的计算成本分别为 $7T_h+3T_{pm}+1T_{fe}$ 和 $23T_h+12T_{pm}+1T_{fe}$，而其他协议[4,5,7~9]在执行注册阶段和认证阶段的计算成本如表 4 所示。其中，一次模糊提取器函数的执行时间等于一次椭圆曲线点乘运算。可以看出本文协议处于中等偏上，在三因子方法中居于上游。



表 4　计算成本和估计时间比较

Table4 Comparison of computation cost and estimated time

协议	注册阶段	登录阶段	总执行时间/s
文献[4]	$7T_h$	$13T_h+4T_{me}$	2.098
文献[5]	$2T_h$	$6T_h+7T_{me}$	3.658
文献[7]	$4T_h$	$12T_h+14T_s+T_{me}$	0.652
文献[8]	$6T_h+4T_{pm}+2T_{bh}$	$18T_h+11T_{pm}+3T_{bp}+1T_{bh}$	1.157
文献[9]	$6T_h+6T_{pm}+4T_{bh}$	$18T_h+12T_{pm}+4T_{bp}+1T_{bh}$	1.373
本文	$7T_h+3T_{pm}+1T_{fe}$	$23T_h+12T_{pm}+1T_{fe}$	1.047

4　结束语

在多服务器环境下，本文提出了一种三因子的远程身份认证协议，三种因子在远程身份认证的整个过程扮演重要角色，显著提高了安全性。形式化证明验证了攻击者无法得到标志、密码、生物特征等信息。另外所提协议在运算开销等方面没有落后于其他协议。未来，本文将在满足基本安全特性的前提下，进一步降低协议的空间和时间复杂度，并考虑将所提协议延展到多种其他环境，例如医疗、云计算等。

参考文献：

[1] 帅青红，苗苗. 网上支付与电子银行 [M]. 北京：机械工业出版社，2015. (Shuai Qinghong, Miao Miao. Online payment and electronic banking [M]. Beijing: Machinery Industry Press, 2015.)

[2] 谭志华. 网络认证协议的高效模型检测研究 [D]. 长沙：湖南大学，2011. (Tan Zhihua. Research on efficient model checking of network authentication protocol [D]. Changsha: Hunan University, 2011.)

[3] Amin R, Islam S H, Biswas G P, *et al.* Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems [J]. Journal of Medical Systems, 2015, 39 (11): 1-21.

[4] Pippal R S, Jaidhar C D, Tapaswi S. Robust smart card authentication scheme for multi-server architecture [J]. Wireless Personal Communications, 2013, 72 (1): 729-745.

[5] Wei Jianghong, Liu Wenfen, Hu Xuexian. Cryptanalysis and improvement of a robust smart card authentication scheme for multi-server architecture [J]. Wireless Personal Communications, 2014, 77 (3): 2255-2269.

[6] 龙丽萍，陈伟建，杨拥军，等. 基于双因子认证技术的 RFID 认证协议的设计 [J]. 计算机工程与设计, 2013, 34 (11): 3726-3730. (Long Liping, Chen Weijian, Yang Yongjun, *et al.* Double factors based authentication protocol for RFID [J]. Computer Engineering and Design, 2013, 34 (11): 3726-3730.)

[7] 张雪，李光松，韩文报，等. 基于身份的跨自治域认证密钥协商协议 [J]. 四川大学学报：工程科学版, 2015, 47 (4): 125-131. (Zhang Xue, Li Guangsong, Han Wenbao, *et al.* Identity-based authenticated key agreement protocol cross autonomous domains [J]. Journal of Sichuan University: Engineering Science Edition, 2015, 47 (4): 125-131.)

[8] 屈娟，李艳平，伍习丽. 对两个基于智能卡的多服务器身份认证方案的密码学分析与改进 [J]. 计算机应用, 2015, 35 (8): 2199-2204. (Qu Juan, Li Yanping, Wu Xili. Cryptanalysis and improvement of two multi-server remote user authentication schemes using smart cards [J]. Journal of Computer Applications, 2015, 35 (8): 2199-2204.)

[9] Choi Y, Nam J, Lee D, *et al.* Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. [J]. Scientific World Journal, 2014, 37 (4): 281-292.

[10] 陈小峰，冯登国. 一种基于双线性映射的直接匿名证明方案 [J]. 软件学报，2010, 21 (8): 2070-2078. (Chen Xiaofeng, Feng Dengguo. Direct anonymous attestation based on bilinear maps [J]. Journal of Software, 2010, 21 (8): 2070-2078.)

[11] 雷奇，尚涛，刘建伟. 基于随机预言模型的量子仲裁签名方案安全性分析 [J]. 密码学报, 2016, 4 (6): 619-628. (Lei Qi, Shang Tao, Liu Jianwei. Security analysis for arbitrated quantum signature scheme based on random oracle model [J]. Journal of Cryptologic Reseatch, 2016, 4 (6): 619-628.)

[12] Tang Yonglong. A user authentication protocol based on multiple factors [J]. Journal of Networks, 2014, 9 (10): 1081-1090.

[13] 杨懿竣. 指纹安全认证的不可逆变换技术研究 [D]. 深圳：深圳大学，2015. (Yang Yijun. Research on irreversible transformation of fingerprint security authentication [D]. Shenzhen: Shenzhen University, 2015.)

[14] Chiou Shinyan, Ying Zhaoqin, Liu Junqiang. Improvement of a privacy authentication scheme based on cloud for medical environment [J]. Journal of Medical Systems, 2016, 40 (4): 101-115.